INTERNATIONAL STANDARDIZED PROFILE

ISO/IEC ISP 15126-2

First edition
1999-04-15

Information technology — International Standardized Profiles FDY1n — Directory data definitions —

Part 2:
FDY12 — Directory system schema

Technologies de l'information — Profils normalisés internationaux FDY1n — Définitions de données de l'Annuaire —

Partie 2: FDY12 — Schéma du système de l'Annuaire

Reference number
ISO/IEC ISP 15126-2:1999(E)

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. In addition to developing International Standards, ISO/IEC JTC 1 has created a Special Group on Functional Standardization for the elaboration of International Standardized Profiles.

An International Standardized Profile is an internationally agreed, harmonized document which identifies a standard or group of standards, together with options and parameters, necessary to accomplish a function or a set of functions.

Draft International Standardized Profiles are circulated to national bodies for voting. Publication as an International Standardized Profile requires approval by at least 75 % of the national bodies casting a vote.

International Standardized Profile ISO/IEC ISP 15126-2 was prepared with the collaboration of

— Asia-Oceania Workshop (AOW);

— European Workshop for Open Systems (EWOS);

— Open Systems Environment Implementors' Workshop (OIW).

ISO/IEC ISP 15126 consists of the following parts, under the general title *Information technology — International Standardized Profiles FDY1n — Directory data definitions*:

— *Part 1: FDY11 — Common directory use (normal)*

— *Part 2: FDY12 — Directory system schema*

Annexes A to C form a normative part of this part of ISO/IEC ISP 15126.

Introduction

The concept and structure of International Standardized Profiles for Information Systems are laid down in the Technical Report ISO/IEC TR 10000. The purpose of an International Standardized Profile is to recommend when and how certain information technology standards shall be used. This International Standardized Profile ISO/IEC ISP 15126-2 specifies application profile FDY12 as defined in the Technical Report ISO/IEC TR 10000-2.

ISO/IEC ISP 15126-2 is one of a set of International Standardized Profiles relating to the Directory (see TR 10000-2) for the '93 standards.

ISO/IEC ISP 15126-2 covers information to be stored within the Directory that is common to a variety of applications.

Directory information may be classified as either:

— user information, placed in the Directory by, or on behalf of, users or

— administrative and operational information, held and managed by the Directory to meet various administrative and operational requirements.

This part of ISO/IEC ISP 15126 is only concerned with the administrative and operational information; user information is profiled by ISO/IEC ISP 15126-1: Common directory use (normal).

This part of ISO/IEC ISP 15126 specifies requirements that are applicable to implementations of DUAs and DSAs. Additionally, these requirements may guide Directory users and administrative authorities in defining their needs for the use of the Directory.

The primary aim of this profile is to define the minimum capabilities that a DUA and a DSA shall have to support for allowing a basic common view of the Directory administrative and operational information. It does this by specifying a minimum set of object classes, attribute types, name forms, structure rules and matching rules to be supported.

This part of ISO/IEC ISP 15126 does not limit DSAs to these minimum capabilities - a DSA that complies with this part of ISO/IEC ISP 15126 and has no additional information handling (storage, retrieval and modification) capabilities may not be adequate for many purposes, and implementors are strongly encouraged to provide such additional capabilities.

This part of ISO/IEC ISP 15126 is harmonized among these three Workshops and it was finally ratified by the Workshops' plenary assemblies.

Information technology — International Standardized Profiles FDY1n — Directory data definitions —

Part 2:
FDY12 — Directory system schema

1 Scope

1.1 General

This part of ISO/IEC ISP 15126 profiles Directory System Schema information to be stored within the Directory. This is the information, common to a variety of applications, which the Directory itself needs to know in order to operate correctly. This information is specified in terms of subentries and operational attributes.

To support the implementation of the Directory as defined by IUT-T Rec. X.500-series | ISO/IEC 9594 edition 1993, this part of ISO/IEC ISP 15126 gives requirements that are applicable to implementations of Directory System Agents (DSAs). Additionally, these requirements may guide Directory users and administrative authorities in use of the Directory.

The primary objective of this part of ISO/IEC ISP 15126 is to define the minimum capabilities that DUAs and DSAs shall support concerning the management and storing of operational and administrative information. It does this by specifying for a conformant DSA a minimum set of requirements concerning the specific tree structure for operational information and the operational content of the entries and subentries.

This part of ISO/IEC ISP 15126 does not limit DSAs to these minimum capabilities - a DSA that complies with this part of ISO/IEC ISP 15126 and has no additional information handling (storage, retrieval and modification) capabilities may not be adequate for many purposes, and implementors are strongly encouraged to provide such additional capabilities.

Therefore, contrary to ISO/IEC ISP 15126-1, this part of ISO/IEC ISP 15126 does not recommend Naming Authorities in any way not to restrict their selection of object classes or naming attributes for operational information to those which are required to be supported by this part of ISO/IEC ISP 15126. Rather, it guarantees that selections made within the scope of this part of ISO/IEC ISP 15126 will be within the capabilities of DSAs compliant with this International Standardized Profile.

Interworking between DSAs which comply with this part of ISO/IEC ISP 15126 will be greatly facilitated on this minimum basis.

Clause 6 deals with Name Forms and Structure Rules which may be used to constrain subentries belonging to a particular subtree. This is done by reference to and within the scope of ITU-T Rec. X.501 | ISO/IEC 9594-2. Subclause 7.1 deals with object classes for subentries. Subclauses 7.2 and 7.3 deal with operational attribute types, content rules for the directory system schema respectively.

The Directory Access Protocol (DAP) and the Directory System Protocol (DSP), as defined by ITU-T Rec. X.500 series | ISO/IEC 9594, can be used to access information stored in a Directory Information Base (DIB) fragment which is profiled by this part of ISO/IEC ISP 15126.

1.2 Position within the taxonomy

This part of ISO/IEC ISP 15126 is identified in ISO/IEC TR 10000-2 as ”FDY12 - Directory data definitions - Directory system schema”.

1.3 Scenario

A Directory user (e.g., an application-process), by means of its associated Directory User Agent (DUA), which has special administrative capabilities, obtains Directory administrative and operational information by accessing directly or indirectly one or more DSAs of the Directory (see figure 1).

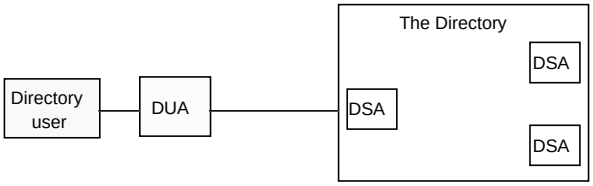

Figure 1 — Access to the Directory

2 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC ISP 15126. At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this part of ISO/IEC ISP 15126 are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by ISPs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and ITU-T maintains published editions of its current Recommendations.

Amendments and corrigenda to the base standards are referenced: see Annex B for a complete list of these documents which are used in this part of ISO/IEC ISP 15126.

2.1 Paired ITU-T Recommendations | International Standards equivalent in technical content

ITU-T Rec. X.500 (1993) | ISO/IEC 9594-1:1995, *Information technology — Open Systems Interconnection — The Directory: Overview of concepts, models, and services.*

ITU-T Rec. X.501 (1993) | ISO/IEC 9594-2:1995, *Information technology — Open Systems Interconnection — The Directory: Models.*

ITU-T Rec. X.511 (1993) | ISO/IEC 9594-3:1995, *Information technology — Open Systems Interconnection — The Directory: Abstract service definition.*

ITU-T Rec. X.518 (1993) | ISO/IEC 9594-4:1995, *Information technology — Open Systems Interconnection — The Directory: Procedures for distributed operation.*

ITU-T Rec. X.519 (1993) | ISO/IEC 9594-5:1995, *Information technology — Open Systems Interconnection — The Directory: Protocol specifications.*

ITU-T Rec. X.520 (1993) | ISO/IEC 9594-6:1995, *Information technology — Open Systems Interconnection — The Directory: Selected attribute types.*

ITU-T Rec. X.521 (1993) | ISO/IEC 9594-7:1995, *Information technology — Open Systems Interconnection — The Directory: Selected object classes.*

ITU-T Rec. X.509 (1993) | ISO/IEC 9594-8:1995, *Information technology — Open Systems Interconnection — The Directory: Authentication framework.*

ITU-T Rec. X.525 (1993) | ISO/IEC 9594-9:1995, *Information technology — Open Systems Interconnection — The Directory: Replication.*

ITU-T Rec. X.680 (1994) | ISO/IEC 8824-1:1995, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation.*

ITU-T Rec. X.681 (1994) | ISO/IEC 8824-2:1995, *Information technology — Abstract Syntax Notation One (ASN.1): Information object specification.*

ITU-T Rec. X.682 (1994) | ISO/IEC 8824-3:1995, *Information technology — Abstract Syntax Notation One (ASN.1): Constraint specification.*

ITU-T Rec. X.683 (1994) | ISO/IEC 8824-4:1995, *Information technology — Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.*

ITU-T Rec. X.690 (1994) | ISO/IEC 8825-1:1995, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).*

ITU-T Rec. X.880 (1994) | ISO/IEC 13712-1:1995, *Information technology — Remote Operations: Concepts, model and notation.*

ITU-T Rec. X.881 (1994) | ISO/IEC 13712-2:1995, *Information technology — Remote Operations: OSI realizations — Remote Operations Service Element (ROSE) service definition.*

ITU-T Rec. X.882 (1994) | ISO/IEC 13712-3:1995, *Information technology — Remote Operations: OSI realizations – Remote Operations Service Element (ROSE) protocol specification.*

2.2 Normative Amendments and Technical Corrigenda

In accordance with TR10000-1 subclause 6.3.2 c), attention is drawn to normative Amendments and Technical Corrigenda affecting the Directory Standards documents IEC 9594:1994 and the ITU-T X.500:1993 recommendations.

It should be noted that references made to these standards are almost always invalid if taken as references to the '88 standards.

Annex B defines the references to the agreed amendments and corrigenda. Compliance with these amendments and corrigenda is necessary to achieve the interoperability requirements for this part of ISO/IEC ISP 15126.

The following subset of these have been identified as particularly relevant to this part of ISO/IEC ISP 15126:

Technical Corrigendum 1 to Recommendation X.501 (1993) | ISO/IEC 9594-2:1995 (addressing DRs 9594/088, 089, 090, 091, 102, 125)

Technical Corrigendum 2 to Recommendation X.501 (1993) | ISO/IEC 9594-2:1995 (addressing DRs 9594/134, 136)

Technical Corrigendum 1 to Recommendation X.511 (1993) | ISO/IEC 9594-3:1995 (addressing DR 9594/085)

Technical Corrigendum 2 to Recommendation X.511 (1993) | ISO/IEC 9594-3:1995 (addressing Defect Reports 9594/119, 133)

Technical Corrigendum 1 to Recommendation X.518 (1993) | ISO/IEC 9594-4:1995 (addressing DRs 9594/094, 106, 108, 109, 111, 112, 113, 114, 115)

Technical Corrigendum 2 to Recommendation X.518 (1993) | ISO/IEC 9594-4:1995 (addressing DRs 9594/116, 117, 118, 119, 120, 121, 130)

Technical Corrigendum 1 to Recommendation X.519 (1993) | ISO/IEC 9594-5:1995 (addressing DRs 9594/075, 124)

Technical Corrigendum 1 to Recommendation X.520 (1993) | ISO/IEC 9594-6:1995 (addressing DRs 9594/076, 122, 127)

Technical Corrigendum 1 to Recommendation X.509 (1993) | ISO/IEC 9594-8:1995 (addressing DR 9594/128)

Technical Corrigendum 2 to Recommendation X.509 (1993) | ISO/IEC 9594-8:1995 (addressing DRs 9594/077, 078, 083, 084)

Technical Corrigendum 3 to Recommendation X.509 (1993) | ISO/IEC 9594-8:1995 (addressing DRs 9594/080, 092, 100)

Technical Corrigendum 1 to Recommendation X.525 (1993) | ISO/IEC 9594-9:1995 (addressing DRs 9594/097, 099, 123)

Technical Corrigendum 2 to Recommendation X.525 (1993) | ISO/IEC 9594-9:1995 (addressing DR 9594/132)

2.3 Additional normative references

ISO/IEC TR 10000-1:1998, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework.*

ISO/IEC TR 10000-2:1998, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 2: Principles and Taxonomy for OSI Profiles.*

ISO/IEC 13248-1:1998, *Information technology — Open Systems Interconnection — The Directory: Protocol Implementation Conformance Statement (PICS) proforma for the Directory Access Protocol.*

ISO/IEC 13248-2:1998, *Information technology — Open Systems Interconnection — The Directory: Protocol Implementation Conformance Statement (PICS) proforma for the Directory System Protocol.*

3 Definitions

3.1 General

Many of the definitions used may be found in the Standards. Since not all of the definitions are to be found in the Definitions clauses within the standards documents, references are listed in Table 1 below. The column "Part" refers to the part number within ISO/IEC 9594 or its ITU-T equivalent (see also clause 2). The column „Reference“ refers to the clause within this part of ISO/IEC ISP 15126.

Table 1 — Definitions and references

Term	Part	Reference
administrative area	2	10.1
autonomous administrative area	2	10.1
specific administrative area	2	10.1
inner administrative area	2	10.1
administrative point	2	10.1
administrative entry	2	10.5.5
user attribute	2	8
operational attribute	2	8
collective attribute	2	8,11.2
subentry	2	11.6
directory system schema	2	13
DSA information model	4	19
DSA-shared attribute	2	19.1
DSA-specific attribute	2	19.1
DSE (DSA specific entry)	2	19.1

3.2 Support Level

To specify the support level of protocol features for this part of ISO/IEC ISP 15126, the following terminology is defined.

3.2.1 Mandatory: "m": Mandatory requirement for support

The support of the feature is mandatory for all implementations claiming compliance with this part of ISO/IEC ISP 15126.

3.2.2 Optional: "o": Optional requirement for support

The support of the feature is left to the implementor of the DSA.

3.2.3 Conditional: "c": Conditional requirement for support

The requirement to support the item depends on a specified condition. The condition and the resulting support requirements are stated separately.

3.2.4 Outside the scope: "i"

Support for the item is outside the scope of this part of ISO/IEC ISP 15126.

3.2.5 not applicable: "-"

The item is not defined in the context where it is mentioned. There is no support requirement. The occurrence of "not applicable" is mainly due to the format of the tables in the ISPICS Requirements List.

4 Abbreviations

Following abbreviations are used as defined in ITU-T Rec. X.500 series | ISO/IEC 9594 or in ISO/IEC TR 10000-1:

AA	Administrative Area
AAA	Autonomous Administrative Area
IAA	Inner Administrative Area
SAA	Specific Administrative Area
AAP	Autonomous Administrative Point
AVA	Attribute Value Assertion
DAP	Directory Access Protocol
DIB	Directory Information Base
DIT	Directory Information Tree
DMD	Directory Management Domain
DMO	Directory Management Organization
DSA	Directory System Agent
DSP	Directory System Protocol
DUA	Directory User Agent
ISP	International Standardized Profile
ISPICS	ISP Implementation Conformance Statement
PRL	Profile Requirements List
RDN	Relative Distinguished Name

5 Conformance

Conformance to this part of ISO/IEC ISP 15126 concerns the type of operational and administrative information which DSAs shall support.

Call for support of a certain type of information (e.g. object classes, attribute types) means that the conforming DSA shall be able to handle the information as described by this part of ISO/IEC ISP 15126.

This ability of a DSA shall be capable of being tested by setting up suitable test suites. The conformance statements of this part of ISO/IEC ISP 15126 lay down the range of information for suitable DSA test suites.

In practice, the behaviour of an actual DSA may depend on multiple conditions, like access control, or schema or other restrictions applied for administrative reasons. Therefore test suites, even if applicable in principle, cannot be performed successfully in all situations. A DSA is conformant according to this part of ISO/IEC ISP 15126 if the DSA, after suitable set-up, is able to successfully carry out test suites within the range of information defined in this part of ISO/IEC ISP 15126.

Note: Suitable set-up is implied within this part of ISO/IEC ISP 15126.

5.1 DSA Conformance

DSA conformance requirements involve

a) the support of the specific DIT structure for operational information as specified in clause 6.

b) the support of object classes as specified in 7.1;

c) the support of operational attribute types as specified in 7.2;

d) the support of the specific content rules for operational information as specified in 7.3.

In addition, a PICS shall be provided stating support or non-support of each option on object classes and attribute types identified in A.6.4, and on name forms and matching rules identified in A.6.5.

The support of the Directory Administrative model is out of scope of this part of ISO/IEC ISP 15126.

The way the DSA information model is implemented, meaning how the DSA stores, accesses and retries DSA information, is out of scope of this part of ISO/IEC ISP 15126.

5.2 DUA conformance

DUA capabilities are necessarily tied to user needs, which may vary. DUAs handling with the Directory System Schema will require special administrative capabilities. Several features can be defined, to which such a DUA may claim conformance:

- A DUA claiming support of an object class shall do it by

a) being able at minimum to carry out rendition of the object class value in a manner appropriate to its user interface. In the context of a DUA for a human, this would mean rendition in a suitable graphic form.

b) being able, if it supports add operations, to include in the request the correct values of the object class attribute, that is the object identifier of the structural object class and of its superclasses.

- A DUA claiming support of an operational attribute type shall do it by

a) being able to create and send the protocol elements necessary to access operational attributes,

b) being able to receive and, in the context of a DUA for a human, to display correctly the attribute values completely and in all defined forms,

c) being able, if it supports modify operations, to generate requests for adding and removing this attribute and its attribute values in all defined forms,

d) being able, if it supports search operations, to use this attribute in a filter component appropriate to the attribute definition and supported matching rules.

e) being able, if it supports such operations, to create a filter with „presence match“.

- A DUA claiming support of a Matching Rule shall do it by

being able to specify this matching rule in a search operation with extensibleMatch.

- A DUA claiming support of the subentry type shall do it by

a) being able to use the implicit structure rules associated with a subentry to compose the DN of a subentry,

b) being able, if it supports modify operations, to use the implicit structure rules associated with subentries for adding a subentry under an administrative entry.

c) being able to set the service controls necessary to access subentries in a Search or a List operation,

d) being able to receive and, in the context of a DUA for a human, to display correctly the attribute types and values of a subentry completely and in all defined forms,

e) being able, if it supports modify operations, to generate requests for adding and removing attributes and attribute values of a subentry.

6 Specific DIT Structure for operational information

This chapter only deals with aspects of the DIT structure concerning administrative and operational information.

The form of the DIT that is relevant for administrative entries and subentries and required by the administrative and naming authorities responsible of a given region/domain/subtree is specified with the help of

- the Name forms, which define which attributes are used to form the RDN of a subentry
- implicit DIT Structure rules, which define the hierarchical relationship of administrative entries and subentries.

6.1 Name forms

Implementations claiming conformance with this part of ISO/IEC ISP 15126 shall support name forms as listed in A.6.5.1.1.

Note : This is in fact only the subentryNameForm.

Support of these name forms by a DSA conformant with this part of ISO/IEC ISP 15126 means that all the following conditions are fulfilled:

a) The DSA supports the named object class as described in 7.1.

b) The DSA is able to create a subentry of specified object class, the RDN of which contains all mandatory attributes and zero or more of the optional attributes indicated in the name form.

6.2 DIT Structure Rules

The Directory System Schema is not regulated with explicit DIT structure rules as defined in ITU-T X.501 | ISO/IEC 9594-2, 12.6.5.

However several structure rules are defined in ITU-T X.501 | ISO/IEC 9594-2, 11.6.1 and concern the placement of subentries within the DIT and the hierarchical relationship of subentries with other entries.

Implementations conformant with this part of ISO/IEC ISP 15126 shall be capable of supporting the specification mechanisms concerning subentries as defined in ITU-T X.501 | ISO/IEC 9594-2, 11.6, and this part of ISO/IEC ISP 15126.

Support of these mechanisms by a DSA conformant with this part of ISO/IEC ISP 15126 means that all the following conditions are fulfilled:

a) The DSA supports the subentry name form as described in 6.1.

b) The DSA is able to create subentries subordinate to all kinds of administrative points,

c) The DSA is able to prevent creation of subentries of a type not allowed by the associated administrative entry,

Note : The creation of a subentry of the object class subschema, accessControlSubentry or collectiveAttributeSubentry is not allowed if the aministrativeRole attribute of the associated administrative entry only has the value id-ar-autonomousArea.

d) The DSA is able to prevent creation of subentries subordinate to an entry which is not an administrative entry,

e) The DSA is able to prevent creation of entries or subentries subordinate to a subentry.

Note : It is possible to transiently have specific administrative entries without associated subentries. This would represent a transient situation.

7 Operational Content of Entries and Subentries

7.1 Object Classes

Standard object classes defined within ITU-T Rec. X.521 | ISO/IEC 9594-7 shall be supported as specified in A.6.4.1.1.

These standard object classes only concern subentries. Within the Directory System Schema, only the content of subentries is regulated by object classes.

Support of these object classes requires the DSA to be able to store, modify and retrieve, via Directory operations, a subentry of its fragment of the DIT, if the subentry is associated with supported object classes and the following conditions are fulfilled:

a) The subentry lies within the DIT as described in 6.1;

b) The subentry contains all mandatory attributes as determined by its object classes - structural and auxiliaries if any;

c) The subentry contains no other than mandatory and optional attributes as defined by its object classes - structural and auxiliaries if any.

Conformant DSAs shall accept subentries which explicitly indicate Top in their object class attribute. Indication of object class Top is optional according to ITU-T X.501 | ISO/IEC 9594-2, 12.3.2.

Support of a standard object class implies support of its mandatory attribute types (see A.6.4.2.1) and support of its optional attribute types (see A.6.4.2.1) for which support is claimed for the DSA.

A conformant DSA shall reject requests for creation or modification of subentries that as a consequence would not fulfil the condition a), b) or c).

In particular, a conformant DSA shall not permit the creation or modification of subentries which contain attributes not identified by any of its object classes or by Content Rules (see 7.3).

7.2 Operational Attribute Types

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support an operational attribute type as follows:

a) The DSA shall perform, on the original inclusion or on a subsequent modification attempt of an attribute, the checking algorithm which is associated with the syntax of the attribute, when required (see FDY11, 7.4);

b) The DSA shall check that the number of attribute values complies with the single-valued element of the attribute definition;

c) The DSA shall check that the attribute value(s) conform with the bounds defined in ITU-T X.501.

d) The DSA shall support the matching rules, if any, that are directly associated with the elements of the attribute type definition or of its supertype attributes, and shall execute these matching rules in a manner that conforms with ITU-T X.520 | ISO/IEC 9594-6, ITU-T X.501 | ISO/IEC 9594-2, 12.5.2 and 20 as clarified in 7.4.

7.2.1 Standard Operational Attributes Types

The operational attribute types listed in A.6.4.2.1 are defined in ITU-T Rec. X.501 | ISO/IEC 9594-2.

They shall be supported as specified in A.6.4.2.1, 7.1, 7.2 and 7.3.

There are several varieties of operational attributes, depending on

- the type of the „entry“ to which they belong (subentry, entry, administrative entry, DSE),
- their role for the DSA operation.

Some operational attributes do not correspond to directory entries.

7.2.1.1 Operational attributes of an administrative entry

Contrary to a subentry, which is a special kind of entry, an administrative entry is not a special kind of entry. It is an entry holding an **administrativeRole** attribute.

But some operational attributes may only be held by administrative entries. These attributes are not associated with any object class.

These are:

- **administrativeRole**
- **accessControlScheme**
- **subentryACI**

The conformance requirements concerning these attributes are described in 7.3.

7.2.1.2 Operational attributes of a subentry

The operational attributes of a subentry are used in conjunction with the standard object classes for subentries specified in A.6.4.1.1, as either mandatory or optional attributes.

These are listed in the following table with their associated object class.

Operational Attributes	Associated object class
subTreeSpecification	subentry
dITStructureRule **nameForms** **dITContentRules** **objectClasses** **attributeTypes** **matchingRules** **matchingRuleUse**	subschema

The conformance requirements for these attributes are described in 7.1 and 7.2.

Other operational attributes of a subentry are not explictly associated with an object class. These are:

- **prescriptiveACI**
- **entryACI**
- **createTimeStamp**
- **modifyTimeStamp**

The conformance requirements concerning these attributes are described in 7.3.

7.2.1.3 Operational attributes of an entry

These attributes are not associated with any object class.

These are:

- **createTimeStamp**
- **modifyTimeStamp**

- **creatorsName**
- **modifiersName**
- **collectiveExclusions**
- **structuralObjectClass**
- **governingStructureRule**
- **entryACI**

The conformance requirements concerning these attributes are described in 7.3.

7.2.1.4 Operational attributes not necessarily associated with entries

Those are the DSA-shared and DSA-specific attributes defined within the DSA information model.

These attributes are:

- **dseType**
- **myAccessPoint**
- **superiorKnowledge**
- **specificKnowledge**
- **nonSpecificKnowledge**
- **supplierKnowledge**
- **consumerKnowledge**
- **secondaryShadows**

Since DAP requests cannot be used for handling these operational attributes, the way these operational attributes are supported is out of the scope of this part of ISO/IEC ISP 15126.

Note : The functionality associated with these operational attributes is profiled in the ISO/IEC ISP 15125-4 (ADY22).

7.2.2 Additional Operational Attribute Types

Administrative Authorities may define additional operational attributes. The use of these operational attributes is local matter.

7.2.3 Collective attributes

No operational attributes are collective.

7.2.4 Attribute Hierarchy

Attribute hierarchy is the capability of deriving attribute subtypes from a generic attribute type called the supertype.

No attribute hierarchy is defined for operational attributes.

7.3 Content Rules for the Directory System Schema

The Directory System Schema is not regulated by explicit DIT content rules.

However several content rules are defined for the Directory System Schema: these specify which operational attributes a subentry or an entry shall or may contain. These requirements are listed in this clause.

7.3.1 Mandatory operational attributes of an administrative entry

7.3.1.1 administrativeRole

The **administrativeRole** operational attribute, as defined in ITU-T X.501 | ISO/IEC 9594-2, 10.5.4, identifies an entry as an administrative entry. The values of this attribute identify the type(s) of an administration point.

An administrative entry may be created while creating a new entry with an administrativeRole attribute, or adding the administrativeRole attribute to an existing entry.

An existing administrative entry may be modified in modifying or adding values of the administrativeRole attribute.

Support of this attribute is conditional, as stated in A.6.4.2.1.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

a) when creating or modifying an existing entry in order to make it an administrative entry, the DSA shall check the values of the administrativeRole attribute and reject the request in the following cases:

- when one or more values do not belong to the list contained in ITU-T Rec. X.501 | ISO/IEC 9594-2, 13.3, except when permitted by a local policy,
- when the administrativeRole attribute contains simultaneously the values id-ar-accessControlSpecificArea and id-ar-accessControlInnerArea,
- when the administrativeRole attribute contains simultaneously the values id-ar-autonomousArea and id-ar-accessControlInnerArea,
- when the administrativeRole attribute contains simultaneously the values id-ar-collectiveAttributeSpecificArea and id-ar-collectiveAttributeInnerArea,
- when the administrativeRole attribute contains simultaneously the values id-ar-autonomousArea and id-ar-collectiveAttributeInnerArea.

b) when modifying an existing administrative entry, adding a value to the attribute administrativeRole, the DSA shall reject the request in the following cases:

- when the Modify request contains an already existing value of the administrativeRole attribute,
- when the modified administrativeRole attribute would contain simultaneously the values id-ar-accessControlSpecificArea and id-ar-accessControlInnerArea,
- when the modified administrativeRole attribute would contain simultaneously the values id-ar-autonomousArea and id-ar-accessControlInnerArea.
- when the modified administrativeRole attribute would contain simultaneously the values id-ar-collectiveAttributeSpecificArea and id-ar-collectiveAttributeInnerArea,
- when the modified administrativeRole attribute would contain simultaneously the values id-ar-autonomousArea and id-ar-collectiveAttributeInnerArea.

c) when modifying an existing administrative entry, removing the value id-ar-accessControlSpecificArea from the attribute administrativeRole, the DSA shall reject the request when it does not remove simultaneously the accessControlScheme attribute.

The administrativeRole attribute may have in addition to the value id-ar-autonomousArea, one or more of the values id-ar-accessControlSpecificArea, id-ar-subschemaAdminSpecificArea or id-ar-collectiveAttributeSpecificArea.

Since the value of the administrativeRole attribute shall not be modified so as to cause existing subentries to become inconsistent, as stated in ITU-T X.501 | ISO/IEC 9594-2, 13.7, the DSA shall only allow removing a value of the administrativeRole attribute if the associated subentry was already removed.

7.3.1.2 createTimeStamp

The **createTimeStamp** operational attribute indicates the time that the administrative entry was created.

Support of this attribute is mandatory.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

When the DSA performs an addEntry operation, it shall create this attribute with the appropriate value in addition to the attributes contained in the addEntry Arguments.

7.3.1.3 modifyTimeStamp

The **modifyTimeStamp** operational attribute indicates the time that the administrative entry or one of its associated subentries was last modified.

Support of this attribute is mandatory.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

a) The DSA shall add this attribute with the appropriate value at least the first time the administrative entry is modified or when creating the first associated subentry. The DSA may already add this attribute when creating the administrative entry.

b) The DSA shall modify the value of this attribute to the appropriate time when modifying the administrative entry or an already existing associated subentry, or when creating a new associated subentry.

Note : The value of the **modifyTimeStamp** of an administrative entry shall always be equal to the value of the **modifyTimeStamp** attribute of the last modified or created associated subentry.

7.3.2 Optional operational attributes of an administrative entry

7.3.2.1 accessControlScheme

The **accessControlScheme** operational attribute, defined in ITU-T Rec. X.501 | ISO/IEC 9594-2, 15.2.2, allows the identification of which access control scheme is in force in a particular portion of the DIT. As stated in ITU-T Rec. X.501 | ISO/IEC 9594-2, 16.3.1, it shall be present if and only if the holding administrative entry is an access control specific entry.

This operational attribute is not allowed for an autonomous administrative entry, the administrativeRole attribute of which only contains the value id-ar-autonomousArea. If this operational attribute is missing with respect to access of a given entry, then the DSA, as stated in ITU-T Rec. X.501 | ISO/IEC 9594-2, 15.2.2 (second note), shall behave as for a 1988 edition DSA.

Note : The absence of this operational attribute in an autonomous administrative entry may be used to designate a part of the tree which has no Access Control applicable to it as a local policy.

Support of this attribute is conditional as stated in A.6.4.2.1.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

a) when creating an administrative entry or modifying it in order to make it an access control specific entry, it means when adding the value id-ar-accessControlSpecificArea to the administrativeRole attribute, the DSA shall check if the request also contains the creation of the accessControlScheme attribute and reject the request if not.

b) the DSA shall reject every add or modify entry request containing an accessControlScheme attribute if this request does not add the value id-ar-accessControlSpecificArea to the administrativeRole attribute.

c) when modifying an existing administrative entry in order to remove the access control specific type, it means when removing the value id-ar-accessControlSpecificArea from the administrativeRole attribute, the DSA shall check if the request also contains the removal of the accessControlScheme attribute and reject the request if not.

d) when modifying an existing administrative entry in order to change the access control type from specific to inner, it means when modifying the value id-ar-accessControlSpecificArea from the administrativeRole attribute in the value id-ar-accessControlInnerArea, the DSA shall check if the request also contains the removal of the accessControlScheme attribute and reject the request if not.

e) the DSA shall only accept for the single value of the operational attribute accessControlScheme one of the values listed in ITU-T Rec. X.501 | ISO/IEC 9594-2, Annex D, or a value permitted by a local security policy.

7.3.2.2 subEntryACI

Subentry ACI attributes are defined as operational attributes of administrative entries, and provide access control information that applies to each of the subentries of the corresponding administrative point. This corresponding administrative point does not need to be an access control specific or inner point, but must otherwise belong to an access control specific, or an access control inner area.

Support of this attribute is conditional as stated in A.6.4.2.1.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

a) when creating an entry which should contain this attribute, the DSA shall check if this will be an administrative entry, it means if the request contains the administrativeRole attribute, and if this entry will belong to an access control specific, or an access control inner area. If both conditions are not fulfilled, the DSA shall reject the request.

b) When modifying an existing administrative entry by adding this attribute, the DSA shall check if this administrative entry belongs to an autonomous, or an access control specific, or an access control inner area and if not reject the request.

Note : Procedures related to the operational attribute **subentryACI** are described in ISO/IEC ISP 15125-9, (ADY45).

7.3.3 Mandatory attributes of a subentry

Some user and operational attributes shall always be present in every subentry; these are the attributes **commonName**, **subtreeSpecification**, **objectClass**, **createTimeStamp** and **modifyTimeStamp**.

Some user and operational attributes shall be present in a subentry, depending on the type of this subentry; these attributes are **prescriptiveACI** and the collective attributes.

7.3.3.1 commonName

Support of this attribute is mandatory.

This attribute shall always be present in every subentry. According to the subentryNameForm (see 6.1), this is the only naming attribute allowed for a subentry.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

When creating a subentry, the DSA shall check if the request contains the commonName attribute. It shall reject the request if not.

7.3.3.2 subtreeSpecification

The operational attribute subTreeSpecification, defined in ITU-T Rec. X.501 | ISO/IEC 9594-2, 11.3.2, allows the definition of the scope of the subentry. It specifies a subset of entries below a specified vertex which forms the base of the subtree or subtree refinement.

Support of this operational attribute is mandatory.

This operational attribute shall always be present in every subentry.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

a) When creating a subentry, the DSA shall check if the request contains the subTreeSpecification attribute. It shall reject the request if not.

b) The DSA shall at least support

- a subtreeSpecification which is an empty sequence, {}. In this case the entries associated with this subentry are all entries contained within the whole administrative area.
- base only, allowing to define a vertex different of the administrative entry,
- and Refinement based on Selection per ObjectClass.

7.3.3.3 objectClass

Support of this attribute is mandatory.

This attribute shall always be present in every subentry.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

a) When creating a subentry, the DSA shall check if the request contains the object class attribute. It shall reject the request if not.

b) When creating a subentry, the DSA shall check the value(s) of the object class attribute within the request. The DSA shall reject the request if it contains a value which is neither id-sc-subentry, nor id-sc-accessControlSubentry, nor id-sc-collectiveAttributeSubentry, nor is-sc-subschemaSubentry.

c) When creating a subentry, the DSA shall check the value(s) of the object class attribute within the request and compare them with the values of the administrativeRole attribute of the associated administrative entry and reject the request in the following cases:

- The request contains for the objectClass attribute the value id-sc-accessControlSubentry, but the administrativeRole attribute of the associated administrative entry does not contain the value id-ar-accessControlSpecificArea or id-ar-accessControlInnerArea,

- The request contains for the objectClass attribute the value id-sc-collectiveAttributeSubentry, but the administrativeRole attribute of the associated administrative entry does not contain the value id-ar-collective AttributeSpecificArea or id-ar-collectiveAttributeInnerArea,

- The request contains for the objectClass attribute the value id-sc-subschemaSubentry, but the administrativeRole attribute of the associated administrative entry does not contain the value id-ar-subschemaAdminSpecificArea.

7.3.3.4 createTimeStamp

The **createTimeStamp** operational attribute indicates the time that a subentry was created.

Support of this attribute is mandatory.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

When the DSA performs an addEntry operation in order to create a subentry, it shall create this attribute with the appropriate value in addition to the attributes contained in the addEntry Arguments.

7.3.3.5 modifyTimeStamp

The **modifyTimeStamp** operational attribute indicates the time that a subentry was last modified.

Support of this attribute is mandatory.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

a) The DSA shall add this attribute with the appropriate value at least the first time the subentry is modified, performing a modifyEntry or a modifyDN operation. The DSA may also add this attribute when creating the subentry.

b) When the DSA modifies again a subentry, performing a modifyEntry or a modifyDN operation, it shall modify the value of this attribute to the appropriate time.

Note : Creating or modifying a subentry affects the value of the **modifyTimeStamp** attribute of the associated administrative entry.

7.3.3.6 prescriptiveACI

The **prescriptiveACI** operational attribute is defined in ITU-T Rec. X.501 | ISO/IEC 9594-2, 16.5.1 and contains access control information applicable to entries within that subentry's scope. As stated in ITU-T Rec. X.501 | ISO/IEC 9594-2, 13.5.1, a subentry of the object class accessControlSubentry shall contain precisely one prescriptive ACI attribute of a type consistent with the value of the accessControlScheme attribute of the corresponding access control specific point.

Note : The prescriptiveACI operational attribute is not mandatory for a subentry associated with an autonomous administrative entry when the object class attribute of this subentry does not have the value id-sc-accessControlSubentry.

This operational attribute is multivalued.

Support of this attribute is conditional as stated in A.6.4.2.1.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

a) When creating a subentry, the DSA shall check the values of the object class attribute within the request. If one value is id-sc-accessControlSubentry, then the add request shall also contain a prescriptiveACI attribute;

The DSA shall reject the request:

- if the request contains the value id-sc-accessControlSubentry for the object class attribute, and no attribute prescriptiveACI,
- or if the request contains one value for the prescriptiveACI attribute, but not the value id-sc-accessControlSubentry for the object class attribute,
- or if the request contains values for the prescriptiveACI which are not consistent with the value of the accessControlScheme attribute of the corresponding access control specific point.

b) When modifying an existing subentry in order to make it an access control subentry, adding the value id-sc-accessControlSubentry to the object class attribute, the DSA shall check the request and reject it if it does not also contain a prescriptiveACI attribute.

Note : Procedures related to the operational attribute **prescriptiveACI** are described in ISO/IEC ISP 15125-9, (ADY45).

7.3.3.7 Collective Attributes

A subentry of object class collectiveattributeSubentry shall contain, as stated in ITU-T Rec. X.501 | ISO/IEC 9594-2, 13.6, at least one collective attribute.

Support of this object class is conditional as stated in A.6.4.2.1.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this object class as follows:

a) When creating a subentry, the DSA shall check the values of the object class attribute within the request. If one value is id-sc-collectiveAttributeSubentry, then the add request shall contain at least one collective attribute;

The DSA shall reject the request:

- if the request contains the value id-sc-collectiveAttributeSubentry for the object class attribute, and no collective attribute,

- or if the request contains one or more collective attributes, but not the value id-sc-collectiveAttributeSubentry for the object class attribute,
- or if the request contains user attributes which are not collective attributes, independently of the value of the object class attribute, except where permitted by local policy.

Note : As an example the user attribute Description may be included in a subentry.

b) When modifying a collective attribute subentry, the DSA shall allow the addition of one or more collective attributes. It shall not allow the addition of one or more user attributes, which are not collective, except where permitted by local policy.

c) When modifying an existing subentry in order to make it a collective attribute subentry, adding the value id-sc-collectiveAttributeSubentry to the object class attribute, the DSA shall check the request and reject it if it does not contain at least one collective attribute.

d) When modifying an existing collective attribute subentry in order to remove the collective attribute type, it means when removing the value id-sc-collectiveAttributeSubentry from the object class attribute, the DSA shall check the request and reject it if it does not simultaneously remove all collective attributes contained in the subentry.

7.3.4 Optional attributes of a subentry

7.3.4.1 entryACI

The use of the attribute entryACI is described in ISO/IEC ISP 15125-9, (ADY45).

7.3.4.2 User Attributes

User attributes are not forbidden in a subentry. A local policy may define which user attributes may be present in a subentry.

Note : Such User attributes could be for instance description or seeAlso.

7.3.5 Attributes excluded from a subentry

The operational attributes **structuralObjectClass** and **governingStructureRule** shall not be present in a subentry.

7.3.6 Mandatory operational attributes of an entry

7.3.6.1 createTimeStamp

The **createTimeStamp** operational attribute is defined in ITU-T Rec. X.501 | ISO/IEC 9594-2, 13.4.1 and indicates the time that an entry was created.

Support of this attribute is mandatory.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

When the DSA performs an addEntry operation, it shall create this attribute with the appropriate value in addition to the attributes contained in the addEntry Arguments.

7.3.6.2 modifyTimeStamp

The **modifyTimeStamp** operational attribute is defined in ITU-T Rec. X.501 | ISO/IEC 9594-2, 13.4.1 and indicates the time that an entry was last modified.

Support of this attribute is mandatory.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

a) The DSA shall add this attribute with the appropriate value at least the first time the entry is modified, when performing a modifyEntry or a modifyDN operation. The DSA may also add this attribute when creating the entry.

b) When the DSA modifies again an entry, performing a modifyEntry or a modifyDN operation, it shall modify the value of this attribute to the appropriate time.

7.3.6.3 creatorsName

The **creatorsName** operational attribute is defined in ITU-T Rec. X.501 | ISO/IEC 9594-2, 13.4.2 and indicates the distinguished name of the Directory user that created an entry.

Support of this attribute is mandatory.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

a) If the Directory user performed a Bind with credentials, then the DSA, performing an addEntry operation, it shall create this attribute with the appropriate value in addition to the attributes contained in the addEntry Arguments. This value is the name of the access control identity defined in ITU-T Rec. X.501| ISO/IEC 9594-2, 15.2.1 and profiled in ISO/IEC ISP 15125-7 (ADY43), 6.10.

b) The case where a Directory User is allowed to perform an addEntry operation within an association using an anonymous Bind is out of scope.

7.3.6.4 modifiersName

The **modifiersName** operational attribute is defined in ITU-T Rec. X.501 | ISO/IEC 9594-2, 13.4.2 and indicates the distinguished name of the Directory user that last modified an entry.

Support of this attribute is mandatory.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

a) When the Directory user performed a Bind with credentials, the DSA shall generate this attribute with the appropriate value the first time an entry is modified by performing a modifyEntry or a modifyDN operation. This value is the name of the access control identity defined in ITU-T Rec. X.501 | ISO/IEC 9594-2, 15.2.1 and profiled in ISO/IEC ISP 15125-7 (ADY43), 6.10.

Note : The DSA may also add this attribute while creating the entry.

b) When another Directory user performed a Bind with credentials and performs another modification to an entry, using a modifyEntry or a modifyDN operation, then the DSA shall modify the value of this attribute to the new distinguished name.

c) The case where a Directory User is allowed to perform a modifyEntry or a modifyDN operation within an association using an anonymous Bind is out of scope.

7.3.7 Optional operational attributes of an entry

7.3.7.1 structuralObjectClass

The **structuralObjectClass** operational attribute is defined in ITU-T Rec. X.501 | ISO/IEC 9594-2, 14.7.8 and indicates the structural object class of the entry.

Support of this attribute is optional.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

When the DSA performs an addEntry operation, it shall generate this attribute with the appropriate value in addition to the attributes contained in the addEntry Arguments. According to ITU-T Rec. X.501 | ISO/IEC 9594-2, 8.1 and 12.6.4, this value shall be the object identifier of the most subordinate object class of the entry's structural object class superclass chain.

7.3.7.2 governingStructureRule

The **governingStructureRule** operational attribute is defined in ITU-T Rec. X.501 | ISO/IEC 9594-2, 14.7.9 and indicates the governing structure rule of the entry.

Support of this attribute is optional.

A DSA claiming conformance with this part of ISO/IEC ISP 15126 shall support this attribute as follows:

a) When the DSA performs an addEntry operation, it shall additionally to the attributes contained in the addEntry Arguments create this attribute with the appropriate value. This is the rule identifier of the DIT structure rule governing the entry.

b) When the DSA performs a modifyDN operation which assigns a new structure rule to the entry, it shall update the value of this attribute to the rule identifier of the new structure rule. The DSA shall also update the value of this attribute in the entries subordinate to the moved entry.

Note : If entries subordinate to the moved entry violate the active subschema, the DSA should make the necessary adjustments to these entries to make them consistent with the subschema.

7.3.7.3 collectiveExclusions

The operational attribute **collectiveExclusions** allows particular or all collective attributes to be excluded from an entry. Support of this attribute is conditional as stated in A.6.4.2.1.

The DSA is not obliged to police the consistency of collectiveExclusions presence and values with the collective attribute policy which may apply for this entry.

Note : Procedures related to the operational attribute **collectiveExclusions** are described in ISO/IEC ISP 15125-3, (ADY21).

7.3.7.4 entryACI

The use of the attribute entryACI is described in ISO/IEC ISP 15125-9, (ADY45).

7.4 Other recommendations

7.4.1 protocolInformation

It is recommended that the **protocolInformation** component is present in the access point information stored and promulgated by a DSA.

Note : Procedures related to the **protocolInformation** component are described in ISO/IEC ISP 15125-4, (ADY22).